

El Centro Criptológico Nacional clasifica sus guías en función de un código numérico que les permite discriminar los asuntos sobre los que versan las mismas. Así pues las guías se distribuyen desde la serie 000 hasta la serie 900, cada una de ella orientada hacia un entorno software o personal distinto y que cada cual debe seleccionar en función de sus atribuciones en la organización que represente.

Así pues las guías se distribuyen en:

- 000 - Guías políticas. Afectan en exclusiva a las administraciones y la implementación que deben desarrollar para disponer de sistemas seguros.
- 100 - Procedimientos. Afectan a todos los destinatarios encargados de implementar los procedimientos de securización de sistemas.
- 200 - Normas. Afectan a quienes deben implementar normas de securización y ejecución en los procedimientos.
- 300 - Instrucciones Técnicas. Afectan a quienes tienen la obligación de implementar las plantillas de securización para hacerlo de forma correcta y normalizada.
- 400 - Guías Generales. Detallan todo tipo de procedimientos sobre herramientas software y hardware que permitan adquirir un grado de securización determinado para la red en la que trabajamos.
- 500 - Guías de entornos Windows. Guías centradas única y exclusivamente en dicho Sistema Operativo en cualquiera de sus versiones de cliente o servidor.
- 600 - Guías de otros entornos. Guías en las que se engloban procedimientos de securización de software y hardware que abarcan desde medios de red hasta software de servicios.
- 700 - Aún sin implementación.
- 800 - Guías del Esquema Nacional de Seguridad. Principios básicos por los que se ha de regir la administración para la protección de la información de la que es generadora y depositaria.
- 900 - Informes Técnicos. Guías que engloban los parámetros de uso y securización de herramientas que permiten elaborar informes técnicos para análisis de vulnerabilidades conocidas.

A pesar de que todas las guías CCN-STIC han sido redactadas para general conocimiento, algunas de ellas han sido restringidas al público en general porque expondrían publicamente configuraciones y parámetros de securización que harían vulnerables los sistemas al ser conocidos con anterioridad,

implementandose el parámetro de "*necesidad de conocer*" que significa que solo tras analizar la petición de un individuo que pretende tener acceso a la información, su responsable determine si es necesario darle acceso a la misma, acotando las personas que pueden acceder a la información restringida. Para la elaboración de dicho sistema la administración se vale de una escala de valores en función de la información a proteger y de los mecanismos necesarios que deben existir para que la información sea protegida. Así pues la escala se ordena de menor a mayor en el siguiente orden y requisitos de acceso y protección.

- SINCLAS = SIN CLASIFICAR
- DIFUSION LIMITADA
- CONFIDENCIAL
- RESERVADA
- SECRETO

En las CCN-STIC el máximo grado de protección existente para dichas configuraciones de software o hardware es **CONFIDENCIAL**, aunque como es lógico hay más de grado **DIFUSION LIMITADA**.

- Las DIFUSION LIMITADA son la 003, 102, 103, 151, 152, 154, 210, 301, 302, 303, 305, 307, 409A, 411, 664, 911A y 911B.
- Y las CONFIDENCIALES son la 150 y 409B.

No se contemplan CCN-STIC bajo el grado de protección de RESERVADO y SECRETO a causa de las importantes medidas de hardware y software que deben ser implementadas para su protección, entrega, cadena de custodia y destrucción.